Internal Audit Report

Payment Card Industry Data Security Standards (PCI DSS) Governance

22 July 2022

Updated with agreed actions June 2023

CS2108

Overall Assessment	Limited Assurance

Contents

This Internal Audit review is conducted for the City of Edinburgh Council under the auspices of the 2021/22 internal audit plan approved by the Governance, Risk and Best Value Committee in March 2021. The review is designed to help the City of Edinburgh Council assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation thereto.

The internal audit work and reporting has been performed in line with the requirements of the Public Sector Internal Audit Standards (PSIAS) and as a result is not designed or intended to comply with any other auditing standards.

Although there are specific recommendations included in this report to strengthen internal control, it is management's responsibility to design, implement and maintain an effective control framework, and for the prevention and detection of irregularities and fraud. This is an essential part of the efficient management of the City of Edinburgh Council. Communication of the issues and weaknesses arising from this audit does not absolve management of this responsibility. High and Critical risk findings will be raised with senior management and elected members as appropriate.

Executive Summary

Overall Assessment	Limited Assurance

Overall opinion and summary of findings

Significant and moderate control weaknesses were identified in the design and effectiveness of the control environment and governance and risk management arrangements established to ensure that the Council achieves compliance with PCI DSS requirements, with instances of non-compliance identified.

Consequently, only limited assurance can be provided that both the Council and associated partner organisations support the secure management of payment channels and cardholder data.

Our review established that the Council currently does not complete its own PCI DSS self-assessment questionnaire (SAQ) to assess compliance across all payment systems used by the Council, and shared drives where payment details could potentially be stored, instead relying solely on the Barclaycard and Worldpay payment provider SAQs to confirm ongoing PCI DSS compliance. As the Council accepts card payment transactions, it is subject to PCI DSS compliance although the handling, collection, processing, and storage of the protected cardholder data is outsourced, and should complete and submit its own annual SAQ in addition to those provided by the Barclaycard and Worldpay to confirm full ongoing compliance.

Additionally, no approved scanning vendor has been appointed by the Council to perform quarterly external vulnerability scans of the Council's networks in line with PCI DSS requirements. Whilst internal network vulnerability scans are performed by CGI (which is an additional PCI DSS requirement), their scope does not currently cover the full PCI Card Data Environment (CDE) requirements detailed in the standards.

Another area of concern relates to the volume of shadow IT applications used across the Council, as it is not currently possible to confirm whether any of these applications support card payment transactions, and (if so) the extent of their compliance with PCI DSS requirements. It is acknowledged that management is currently identifying the full population of shadow IT applications used and has implemented additional procurement controls to ensure that future purchases are identified and recorded.

We also noted that external website providers are sub-contracted by CGI to develop webpages that can include payment processes. Where this is the case, it is important to ensure that contractual arrangements agreed between CGI and the supplier include the requirement to ensure that website security controls are, and remain, aligned with PCI DSS requirements.

It is likely that these gaps have occurred as the Council's PCI DSS governance and risk management arrangements also need to be improved, with responsibilities for ensuring full end to end PCI compliance clearly defined and allocated, and ongoing compliance oversight provided by an appropriate governance forum.

The main risk associated with these findings is potential application of penalty fees and increased transaction fees by the acquiring bank (the Council's bank) where non-compliance and data breaches are identified. These penalties would be applied to the Council and can only be passed to third party payment providers where they are directly responsible for the compliance and / or data breaches. The Council would also require engaging a PCI Forensic Investigator (PFI) to establish the source of the breach which would incur additional costs.

There would also be potential reputational consequences in the event of breaches if citizens lose confidence in the Council's ability to protect their sensitive payment card information, with increased demands for alternative cash payment processes.

Management Response

The Council's Treasury Manager has historically been responsible for PCI DSS compliance.

Given the complexities associated with addressing findings and the need for collaboration across a number of services to agree ongoing ownership and responsibilities for the PCI DSS framework, a phased implementation approach will be adopted.

An implementation plan will be prepared by Treasury and Digital Services for development of a PCI DSS Council wide framework that considers and addresses (where possible) the IA recommendations included in this report and will be agreed with all services and external stakeholders who will be required to support the process.

The plan will be shared with Internal Audit to confirm that appropriate actions have been defined, or risks accepted (where appropriate), and management actions will then be agreed based on the content of the plan, with their implementation progress monitored through the established Internal Audit follow-up process

Audit Areas	Findings	Priority Rating
• Governance and Oversight • Supplier Management	1.Payment Card Industry Data Security Standards (PCI DSS) Governance Arrangements	**High**
• Change Management •Asset Management	2. Third party contracts and supplier management	**Medium**
• Physical Security	3. Alignment between CGI contractual and PCI DSS requirements	**Medium**
• Cardholder Data (CHD) incident management	4. Point of Sale Device Security and Currency	**Medium**

Areas of good practice
The following areas of good practice have been identified: • **Change Management Process** – there is a requirement for completion of data privacy impact assessments (DPIAs) for all planned significant process and technology changes to identify potential data privacy and security risks, with recommendations provided to ensure that they are addressed. • **Shadow IT Applications** – the Council is in the process of identifying its full population of shadow IT applications and has implemented additional procurement controls to ensure that future purchases are identified and recorded. • **Management of Asset Registers** - the council maintains asset registers for point of sale (PoS) devices procured through the Barclaycard and Worldpay that include their location; service owners; model details; and relevant payment provider, satisfying Requirement 9.9.1 of the PCI Standards.

Background and scope

The Payment Card Industry Data Security Standards (PCI DSS) are the information security standards for organisations that accept card payments from major payment card providers such as Visa, MasterCard, Discover, JCB and American Express. Any organisation that accepts card payments must be compliant with PCI DSS standards to demonstrate that Cardholder Data (CHD) and other sensitive financial information is stored, processed and used securely.

PCI DSS consists of the following 12 requirements covering the security controls that interact with, or could otherwise impact the security of, CHD:

1. Protect your system with firewalls
2. Configure passwords and settings
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software
6. Regularly update and patch systems
7. Restrict access to cardholder data to business need to know
8. Assign a unique ID to each person with computer access
9. Restrict physical access to workplace and cardholder data
10. Implement logging and log management
11. Conduct vulnerability scans and penetration tests
12. Documentation and risk assessments

It is essential to maintain PCI DSS compliance to secure cardholder data where it is captured at the point of sale as it flows into the payment system, and to ensure that security threats and vulnerabilities are identified and addressed. This includes protecting card readers; point of sale terminals; networks and wireless access points; data storage and transmission infrastructure; paper-based records; and online payment applications.

PCI DSS Management across the Council

The Council's Treasury Manager is responsible for the Council's PCI DSS compliance, with the Council's main payment gateway (Barclaycard) and associated payment Chip and Pin devices with relevant services responsible for providing ongoing compliance guidance to their own teams.

The Treasury Manager is can also liaise with the Digital Services team and their technology partner CGI for ongoing technical support and guidance.

Some Council services use other payment gateways, including Culture and Wellbeing within the Place directorate for booking tickets; Parking payments (this system is provided by a third party supplier); and the Gov.UK Pay system, which is used across the UK public sector to take payment for services and issue refunds.

Management has confirmed that an historic policy decision was taken that the Council would not hold any CHD to reduce the risks associated with potential non PCI DSS compliance.

Instead, all relevant CHD is acquired and managed under contractual arrangements with Barclaycard, and the Treasury Manager manages the Barclaycard supplier relationship.

The Council's Externally Hosted "Cloud and Web" Services Protocol also confirms that there is no expectation for core Council systems to store credit card details requiring detailed PCI DSS compliance; that Council processes for accepting card payments must be compliant with PCI DSS; and that any externally hosted services that do hold CHD on the Council's behalf do need to be compliant with PCI DSS regulations.

Ongoing PCI DSS compliance is achieved by ensuring that appropriate redirection to the relevant Barclaycard hosted payment pages set up by the Council but owned by Barclaycard incorporated into online payment forms included in the Council's external website. When ready to accept payment details, a URL link is accessed, and card payment details taken securely by Barclaycard, with a success or failure message generated on return to the payment form.

Mail and telephone order (MOTO) payments processed in the Customer Contact Centre are managed through the 'Red Box' telephony application where the telephone recording drops off to enable secure provision of payment card details to Barclaycard, and then re-engages.

Physical payments are collected through BarclayCard and WorldPay chip and pin point of sale devices that do not acquire or store CHD. A significant project was completed in December 2021 that migrated all online and telephony payments to the new Barclay card payment gateway (Smartpay Fuse).

Current Compliance

Management has confirmed that the Council completed a PCI DSS self-assessment in 2020/21 with Barclaycard and has also received confirmation of Barclaycard's own compliance with the standards (September 2021).

Future Plans

Replacement of all legacy Worldpay chip and pin devices (mainly used in educational and cultural venues) with Barclaycard terminals is planned.

Scope

The objective of this review was to assess the adequacy and effectiveness of the key controls established to ensure ongoing compliance with PCI DSS requirements designed to protect cardholder data that is acquired through the Council's website and Customer Contact Centres and processed, transmitted and stored by Barclaycard on behalf of the Council.

Risks

The review aims to provide assurance that the following Council enterprise risks are being effectively managed:

- Supplier, Contractor, and Partnership Management
- Technology and Information
- Governance and Decision Making
- Regulatory and Legislative Compliance
- Fraud and Serious Organised Crime

Limitations of Scope

The following areas were excluded from scope:

- Review and testing of the configuration of network security controls such as firewalls, routers and other network infrastructure, as these areas were covered in the Network Management audit completed in August 2021.
- Security controls in place in shadow IT applications provided by third parties that are not managed by the Council's technology partner CGI.

Reporting Date

Our audit work concluded on 21 July 2022, and our findings and opinion are based on the conclusion of our work as at that date.

Findings and Management Action Plan

Finding 1 – PCI DSS Governance Arrangements

Finding Rating	High Priority

The Council currently has no established governance arrangements to confirm ongoing compliance with PCI DSS requirements. The Treasury team currently manages relationships with the Council's payment partners (Barclaycard and Worldpay) and directs any PCI and payment card queries to either Digital Services, or CGI, however, these responsibilities have not been formally clarified or confirmed. Consequently:

1. Payment channels - the Council cannot confirm its full population of payment channels due to the volume of shadow IT systems historically procured by services that potentially include payment processes and are not supported by Digital Services and CGI.
2. Compliance assessments - PCI DSS compliance self-assessment questionnaires (SAQs) are received annually from the BarclayCard and WorldPay payment providers, however, there is currently no set schedule for completing these annual questionnaires.
3. Compliance assessments – the Council does not complete its own SAQs in addition to those completed by the payment providers to demonstrate ongoing annual PCI DSS compliance.
4. External Vulnerability Scans – an approved scanning vendor has not been appointed to complete quarterly external vulnerability scans, or scans of the Council's networks following significant changes in line with PCI DSS requirement 11.2.2, and 11.2.3.
5. PCI documentation - details of payment channels and payment processes are not consistently maintained. Payment channel information is established when designing and implementing new payment gateways (for example, the project documentation on Barclaycard), but is not maintained to reflect any subsequent changes to operational payment processes.
6. Incident management - response plans for managing PCI related security incidents across all systems (including Shadow IT applications) that accept and process payments have not been created.
7. Risk management - the risks associated with handling; managing; and transferring card holder data (CHD) and other sensitive payment information are not recorded in relevant service risk registers. It is expected that this would include the risks associated with mishandling / misusing CHD; collecting CHD over the phone; and transferring CHD through shadow IT systems.
8. Training and awareness - training on PCI requirements (including security requirements and handling of payment card data) has not been provided to all employees who handle customer payment card details in line with PCI requirements 9.9.3 and 12.6. Guidance on handling point of sale (PoS) devices is provided for some services, however, this is informal.

Risks

- **Governance and Decision Making** - unable to confirm ongoing compliance and PCI DSS risks, and incidents are effectively managed.
- **Regulatory and Legislative Compliance** - non-compliance with requirements in relation to quarterly external vulnerability scanning.
- **Financial and Budget Management** - risk of non-compliance fees applied by relevant payment card brands.
- **Reputational Risk** – adverse publicity associated with PCI DSS breaches

Recommendations and Management Action Plan: PCI DSS Governance Arrangements

Ref.	Recommendation	Agreed Management Action	Owner / Lead Officers	Timeframe
1.1.1	Appropriate Payment Card Industry Data Security Standards (PCI DSS) governance arrangements should be established, with responsibility for ongoing compliance responsibilities allocated to an appropriate Executive and Service Director. A Responsible Officer should be identified as the lead for PCI DSS compliance. One potential governance solution could include extending the responsibility of the established Cyber and Information Security Steering Group (CISSG) to include PCI DSS compliance.	a) An appropriate Responsible Officer will be allocated responsibility for PCI DSS related compliance and their job description would be updated to reflect this responsibility. b) CISSG will be established as the governance forum for PCI-DSS compliance, and all relevant changes and documentation will be approved by CISSG. c) Digital Services will add to the standard agenda and Finance will establish appropriate attendee at CISSG for this.	Deborah Smart, Executive Director of Corporate Services Nicola Harvey, Service Director - Customer & Digital Services Hugh Dunn, Service Director - Finance & Procurement Alison Henry, Head of Corporate Finance (1.1.1a and 1.1.1c) Heather Robb, Chief Digital Officer (1.1.1b) Alison Roarty, Digital Services Commercial & Risk Lead	31/10/23
1.1.2	A RACI matrix that details those within the Council responsible; accountable; to be consulted; and informed should be prepared that describes PCI governance and compliance responsibilities, including completion of self-assessment questionnaires by both the Council (if required) and payment providers.	RACI Matrix will be produced for both CGI and Shadow IT and presented to CISSG for approval.		31/10/23
1.1.3	Current incident response plans should be reviewed to ensure appropriate responsibilities for assigning council and CGI colleagues to triage; manage; and remediate security incidents that impact payment information and assets are in place.	Existing incident response plans for security incidents for both CGI and Shadow IT will be updated to cover security incidents impacting payment information and assets. Role of Finance team will be discussed and updated in these plans.		31/10/23

1.1.4	Relevant risks associated with PCI compliance should be identified; assessed; recorded in relevant service risk registers; and managed, with the most significant risks escalated to the new PCI DSS governance forum.	PCI compliance risks will be identified and recorded in (Finance/Digital Services / Service area) risk registers, and managed/ communicated through CISSG.		31/12/23
1.2.1	An assessment should be performed to determine the full population of payment channels used across the Council, including payments processed using any shadow IT applications, but excluding transactions processed by external payment providers. Note that a register of the shadow IT applications used across the Council is currently being established and will be maintained by Commercial and Procurement Services. This could be used as a reference point.	Assessment is currently underway, and the results of assessment will be documented to include full population of payment channels used across the Council, along with a nominated officer for each channel.	Deborah Smart, Executive Director of Corporate Services Nicola Harvey, Service Director - Customer & Digital Services Hugh Dunn, Service Director - Finance & Procurement Alison Henry, Head of Corporate Finance Heather Robb, Chief Digital Officer Alison Roarty, Digital Services Commercial & Risk Lead	31/10/23
1.2.2	The payment processes and channels identified should be appropriately documented to include detailed payment collection methods (for example, point of sale / online / telephone order) for each channel, together with volumes of annual payment transactions.	CISSG will request the nominated officer for each payment channel to draft payment channel documentation, including: a) payment processes applicable for each payment channels b) payment collection methods (for example, point of sale / online / telephone order), and the volume of annual payment transactions. CISSG will review and approve this documentation.		31/12/23
1.2.3	Digital Services / Commercial and Procurement Services should provide details of all registered shadow IT procurement	Complete as per recommendation.		30/09/23

	approvals for applications that include payment channels to colleagues responsible for ongoing PCI DSS compliance, to ensure that the full population of Council payment channels is completely and accurately maintained.		Deborah Smart, Executive Director of Corporate Services Nicola Harvey, Service Director - Customer & Digital Services Hugh Dunn, Service Director - Finance & Procurement Alison Henry, Head of Corporate Finance Heather Robb, Chief Digital Officer Alison Roarty, Digital Services Commercial & Risk Lead	
1.2.4	The Council should complete its own annual self-assessment questionnaire (SAQ) (in addition to those provided by external payment providers) in line with PCI DSS SAQ guidance to confirm ongoing PCI DSS compliance, and should engage with the payment providers and the acquiring bank (the Council's bank) to determine whether SAQ A (for use of websites that redirect to collect payment providers) and SAQ B (for use of point of sale terminals) should be completed.	By communication through CISSG and known contacts for systems, system owners will be advised to complete the questionnaire. Nominated Officer will review completed questionnaires, compile them into a Council's comprehensive annual SAQ along with details of any potential security gaps, and submit to CISSG for review and approval.		31/12/23
1.2.5	An approved scanning vendor should be appointed to complete quarterly external vulnerability scans in line with PCI DSS requirements 11.2.2 and 11.2.3.	In line with industry best practice, annual scans will be undertaken for all payment systems. CGI or Council framework contract (set up by Digital Services) can be used. The relevant system owners will be responsible for this and any associated costs.		31/03/24
1.3.1	PCI DSS training should be commissioned and delivered to all employees who handle payment transactions in line with PCI requirements on secure handling of payment data and cards. The training materials should include (but not be limited to) common threats associated with payment collection and processing, such as e-skimming and the risks associated with tampering with point of sale (PoS) devices.	The Responsible Officer will work with L&D colleagues to commission a training module through established Council training channel.		31/03/24

Finding 2 – Third party contracts and supplier management

Finding Rating	Medium Priority

CGI Third Party Supplier Management

Where services procure external website providers to develop webpages for Council services, and establish contracts to support ongoing hosting arrangements, CGI may become involved in ensuring that payment interfaces are built that redirect payments to the BarclayCard or WorldPay pages for payment collection, avoiding the need for the Council to collect; process; or store any cardholder payment data. These external relationships are then either managed by services, or CGI on behalf of the Council and include:

- The experience outdoors; joinedinedinburgh; active schools; and mobile pay websites were independently sourced by services who manage ongoing website hosting directly with these external providers. CGI involvement was developing the Barclaycard payment interface for these websites.
- Planning and Building Standards – this is a Scotland wide portal which was developed by the Scottish Government (SG), with only the Barclaycard payment interface being jointly developed by the SG and CGI for the Council.
- Verint / Redbox – the Verint customer relationship management (CRM) system and Redbox solution (used to prevent recording of payment details) is managed by both CGI and their subcontractor Commsworld.
- Gov.pay – this payment system is an addition to the Verint CRM system. The system is provided and managed by the UK Government.
- Parking – NSL provides the web-based systems used to support payment of parking fees and charges.

Our review of a sample of these contracts confirmed that:

- whilst these contracts include information security requirements, they are not fully aligned with PCI DSS security requirements.
- there are no contractual requirements for external suppliers and / or CGI to maintain security controls that are aligned with PCI DSS requirements for the systems referred to above.

CGI has established compensating controls (for example ongoing vulnerability scanning and security monitoring through the established Security Operations Centre) that should be able to identify any potential security threats or issues that arise from these third party hosted web pages. Third party sites in this instance, are the council sites that are built by third party web developers where CGI were involved for onboarding and management.

Shadow IT Payment Services

Whilst the full population of shadow IT applications currently used by the Council to accept payments is currently unknown, existing guidance on procurement contracts and ongoing management of shadow IT applications does not highlight the need to ensure both initial and ongoing compliance with PCI DSS requirements where payments are accepted via shadow IT systems

Risks

- **Supplier, Contractor and Partnership Management** - guidance on supplier contracts and ongoing supplier management does not include the requirement to consider ongoing PCI DSS compliance.
- **Technology and Information** - weaknesses in supplier's infrastructure that could potentially compromise the redirect to payment providers, or that the website providers do not inadvertently store; process; or misuse payment card data.
- **Regulatory and Legislative Compliance** - the council does not currently meet the following PCI DSS requirements:
- **Financial and Budget Management** - potential risk of non-compliance fees applied by relevant payment card brands.
- **Reputational Risk** – adverse publicity associated with PCI DSS breaches.

Recommendations and Management Action Plan: Third party contracts and supplier management

Ref.	Recommendation	Agreed Management Action	Owner / Lead Officers	Timeframe
2.1.1	The established CGI and relevant third-party provider contracts should be reviewed and updated to include: • responsibility for ensuring that third party security arrangements for websites that include redirection links to payment providers are appropriately secured in line with established PCI DSS security requirements.	CISSG will request relevant owners of each payment system involving third party contracts to update those contracts and include responsibility for ensuring that redirection links to payment providers are appropriately secured in line with PCI DSS requirements. Directorates will be responsible for ensuring the system owners provide updates as required.	Deborah Smart, Executive Director of Corporate Services Nicola Harvey, Service Director - Customer & Digital Services Hugh Dunn, Service Director - Finance & Procurement Heather Robb, Chief Digital Officer Alison Roarty, Digital Services Commercial & Risk Lead	31/12/25
2.1.2	Owners for the relevant systems should ensure that all risks associated with ongoing assurance from third parties on their PCI DSS security arrangements are considered, recorded, managed, and mitigated in line with the Council's risk management framework and risk appetite. Where risks cannot be mitigated to an acceptable level this should be escalated to the relevant directorate risk committee, and CLT if required.	System owners will review risks and record the assessment, controls, and mitigating actions.		31/03/24
2.2.1	Existing guidance on procurement contracts and ongoing management of shadow IT applications should be updated to reinforce the need to: ensure that procurement contracts for all shadow IT applications currently used by the Council to accept payments include the requirement to implement and maintain security arrangements that are aligned with PCI DSS standards.	Existing guidance will be updated. Consideration will be given to using this or the DPA Process and evidence presented to IA.		31/10/23

2.2.2	Obtain ongoing assurance from third parties that their security arrangements remain aligned with PCI DSS requirements and provide confirmation of ongoing third-party compliance to colleagues responsible for ongoing PCI DSS governance.	As 2.1.2 Existing guidance will be updated. Consideration will be given to using this or the DPA Process and evidence presented to IA.		31/03/25

Finding 3 – Alignment between CGI contractual and PCI DSS requirements

Finding Rating	Medium Priority

Whilst services provided by CGI to the Council are aligned with some aspects of PCI DSS requirements (for example, managing firewall configuration; network access controls; external connections; whitelisting connections; and formal security change management processes) they are not fully aligned with the following requirements:

- Discovery exercises to identify card holder details inadvertently stored in Council network folders or applications or data stores;
- Quarterly internal vulnerability scans (or scans following implementation of significant changes) and annual penetration tests that cover the full PCI Card Data Environment (CDE) requirements, such as connections between point of sale devices and payment gateways accessed via the Council's networks as required by PCI DSS requirement 11.2.1; 11.2.3; and 11.3.1.

Quarterly wireless analyser scans to detect and identify all authorised and unauthorised wireless access points as required by PCI DSS requirement 11.1 (1 – 2).

Risks

- **Technology and Information** - unauthorised wireless access points and vulnerabilities in connections between point of sale devices and payment gateways are not identified and remediated
- **Regulatory and Legislative Compliance** - the council does not meet PCI DSS security requirements.
- **Financial and Budget Management** - potential risk of non-compliance fees applied by relevant payment card brands.
- **Reputational Risk** – adverse publicity associated with PCI DSS breaches.

Recommendations and Management Action Plan: Alignment between CGI contractual and PCI DSS requirement

Ref.	Recommendation	Agreed Management Action	Owner / Lead Officers	Timeframe
3.1.1	The established CGI contract should be reviewed and updated to: • ensure that CGI contractual and PCI DSS security requirements are consistently aligned with completion of quarterly internal vulnerability scans (or scans following significant change) and annual penetration tests that cover the full PCI card data environment in line with PCI DSS requirements 11.2.1; 11.2.3; and 11.3.1.	Digital Services will ensure that, where CGI already have obligation for PCI-DSS compliance, annual penetration testing will take place.	Deborah Smart, Executive Director of Corporate Services Nicola Harvey, Service Director - Customer & Digital Services	31/03/24

3.1.2	Establish a PCI DSS security breach reporting process where breaches are reported to the relevant PCI DSS governance forum.	Security breach reporting process will be documented, approved by CISSG and communicated to CGI and payment card system owners. Security breaches related to payment cards will be reported through CISSG.	Hugh Dunn, Service Director - Finance & Procurement Heather Robb, Chief Digital Officer Alison Roarty, Digital Services Commercial & Risk Lead	31/12/23
3.1.3	Request CGI to provide annual assurance on compliance with PCI DSS requirements to support submission of Council annual self-assessment questionnaire	We will identify where CGI have contractual obligation for PCI-DSS and work with system owners to ensure that CGI support the annual assessments. System owners will be requested to do the same for the different payment systems.		31/03/24

Finding 4 – Point of Sale Device Security and Currency

Finding Rating	Medium Priority

1. **Secure Point of Sale Connectivity** - the security of point of sale (PoS) connections that connect to Barclaycard and Worldpay through independent wifi routers that are not managed by CGI cannot be confirmed as they have not been independently tested.

   Management has advised that it is Barclaycard and Worldpay's contractual obligation to ensure that these devices connect securely to their hosts.

2. **Unapproved PoS models** -Some PoS models used by the Council (IWL250, iCT200, vx680 and vx820) are not listed in the PCI approved PTS device list.

   Whilst PCI DSS does not specify that only PCI PTS-approved devices can be used, some payment brands (for example VISA or Mastercard) have their own requirements for using PTS-approved devices, including whether PTS devices with expired approvals can be used.

3. **Physical security controls** - physical security controls that should be applied consistently to safeguard PoS devices (for example, securing in locked cabinets) have not been defined and documented, in contravention of Requirements 9.9.3 and 12.6.

Risks

- **Technology and Information** - risk of point of sale (PoS) device firmware being open to exploitation by hackers as no tests or scans have been performed to confirm that they are running on up-to-date patches and security controls. In addition, non-approved devices may not be fit for purpose or may have an inherent fault meaning they are at a higher security risk level as they may not be able to withstand the latest generations of attacks. This risk is exacerbated as non-approved devices do not receive ongoing maintenance and service updates from the payment provider.
- **Fraud and Serious Organised Crime** - unsecured PoS assets could be stolen or used inappropriately
- **Regulatory and Legislative Compliance** - the council does not currently meet the PCI DSS requirements
- **Financial and Budget Management** - potential risk of non-compliance fees applied by relevant payment card brands (for example VISA or Mastercard).
- **Reputational Risk** – adverse publicity associated with PCI DSS breaches

Recommendations and Management Action Plan: Technical configuration of network and network devices

Ref.	Recommendation	Agreed Management Action	Owner / Lead Officers	Timeframe
4.1.1	The implementation plan developed by Treasury and Digital Services should set out responsibilities for ongoing PCI DSS governance activities including: Request payment providers (Barclaycard and Worldpay) to provide ongoing assurance that point-of-sale devices (PoS) are running on the latest software.	Finance and Digital Services will work together to set out the governance responsibilities. System Owners will be required to provide evidence of software update plans by system providers.	Deborah Smart, Executive Director of Corporate Services Nicola Harvey, Service Director - Customer & Digital Services	30/06/2024

	Payment providers should be pushing software updates out to devices as part of their ongoing compliance activities, but it is recommended that the Council obtains ongoing assurance in this area.		Hugh Dunn, Service Director - Finance & Procurement Alison Henry, Head of Corporate Finance Heather Robb, Chief Digital Officer Alison Roarty, Digital Services Commercial & Risk Lead Innes Edwards, Principal Treasury & Banking Manager	
4.1.2	Engage with merchant acquirers or payment brands to advise them of the expired PoS devices currently in use and discuss potential implications.	Finance will engage with merchant acquirers or payment brands to advise them of the expired PoS devices currently in use and discuss potential implications.		01/04/24
4.1.3	Develop plans to replace all non-approved PoS devices currently used by the Council.	Finance will develop plans to replace all non-approved PoS devices currently used by the Council.		31/03/24
4.1.4	Confirm whether new payment devices are approved versions in line with the PCI PTS listing and determine when approvals expire.	Finance will confirm whether new payment devices are approved versions in line with the PCI PTS listing and determine when approvals expire		31/03/24

Appendix 1 – Control Assessment and Assurance Definitions

Overall Assurance Ratings	
Substantial Assurance	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable Assurance	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited Assurance	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
No Assurance	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.

Finding Priority Ratings	
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.
Low Priority	An issue that results in a small impact to the achievement of objectives in the area audited.
Medium Priority	An issue that results in a moderate impact to the achievement of objectives in the area audited.
High Priority	An issue that results in a severe impact to the achievement of objectives in the area audited.
Critical Priority	An issue that results in a critical impact to the achievement of objectives in the area audited. The issue needs to be resolved as a matter of urgency.